

U.S. Application No. 09/685,026
Docket No. YOR920000165US1
(YOR.203)

10

REMARKS

Claims 1, 3, 5-8, and 11-28 are all the claims presently pending in the application.

While Applicant believes that all of the patentable over the prior art of record, to expedite prosecution, claim 1 has been amended to incorporate the features of claims 4, 9, and 10. No new matter is added.

It is noted that the claim amendments are made only for more particularly pointing out the invention, and not for distinguishing the invention over the prior art, narrowing the claims or for any statutory requirements of patentability. Further, Applicant specifically states that no amendment to any claim herein should be construed as a disclaimer of any interest in or right to an equivalent of any element or feature of the amended claim.

Claims 1 and 3-28 stand rejected on prior art grounds.

Claims 1, 3-9, 13-18, 20-22, and 24-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Urata (U.S. Patent No. 6,799,272) in view of Corcoran (David Corcoran, Muscle Flexes Smart Cards into Linux, Source Linux Journal archive, August 1998, Article No. 8), and further in view of Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," Second Edition, pps. 466-474 (hereinafter Schneier).

Claims 10-12, 19, and 23 are rejected under 35 U. S. C. 103(a) as being unpatentable over Urata (US '272) in view of Corcoran (Muscle Flexes Smart Cards into Linux) and Schneier, and further in view of Maillard et al. (U.S. Patent No. 6,466,671).

These rejections are respectfully traversed in the following discussion.

U.S. Application No. 09/685,026
Docket No. YOR920000165US1
(YOR.203)

11

I. THE CLAIMED INVENTION

The claimed invention relates to a method and system for producing wise cards.

In an illustrative, non-limiting embodiment of the invention, as defined by independent claim 1, a method of preventing counterfeiting of a smart card includes providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined small number of readings, wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof.

In conventional methods and systems, counterfeiting/duplication is not rendered difficult since confidential information is carried on the card and an unscrupulous person may find the information simply by looking at or reading the energy construction inside of the card. That is, with a plurality of readings of the card, the information held within the card can be easily detected (e.g., see specification at page 3, line 19, to page 4, line 2).

The claimed invention, on the other hand, complements the conventional smart-card-type of security, which is often all carried on the card itself, by providing extra protection depending on cryptography, with the cryptographic structure (e.g., a key) not being carried by the card and which cannot be accessed completely by a predetermined small number of readings. Moreover, the cryptographic structure can only be built by whoever emits the card or the agent thereof (e.g., see specification at page 4, lines 9-13).

The claimed invention, in addition to preventing the creation of false cards different from the legitimate ones, also prevents the fabrication of clones of a given legitimate smart card. That is, the present invention also provides a mechanism of protection designed to

U.S. Application No. 09/685,026
Docket No. YOR920000165US1
(YOR.203)

12

prevent and/or discourage both copying and creation of new cards (e.g., see specification at page 4, lines 14-17).

II. THE PRIOR ART REJECTIONS

Claims 1, 3-9, 13-18, 20-22, and 24-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Urata in view of Corcoran, and further in view of Schneier. Claims 10-12, 19, and 23 are rejected under 35 U. S. C. 103(a) as being unpatentable over Urata in view of Corcoran and Schneier, and further in view of Maillard.

Applicants respectfully submit, however, that it would not have been obvious to combine the cited references in the manner alleged in order to arrive at the claimed invention. Moreover, Applicants submit that there are elements of the claimed invention which are not disclosed or suggested by prior art of record, either individually or in combination. Therefore, Applicants respectfully traverses these rejections.

While Applicant believes that all of the patentable over the prior art of record, to expedite prosecution, claim 1 has been amended to incorporate the features of claims 4, 9, and 10.

The claimed invention has recognized that the unique combination of the features of the claimed invention provides important advantages over the prior art of record, including such teachings as disclosed by each of the individually cited references, Urata, Corcoran, Schneier, and Maillard.

In stark contrast to each of the cited prior art of record, the present invention provides a novel and unobvious method of preventing counterfeiting (i.e., false smart cards or

U.S. Application No. 09/685,026 13
 Docket No. YOR920000165US1
 (YOR.203)

illegitimate cards) and/or preventing cloning (i.e., copies of legitimate smart cards or counterfeit smart cards) of a smart card by authorizing (e.g., verifying the legitimacy of) the smart card. That is, the claimed invention provides a simple and effective solution to problems with conventional smart cards which use cryptographic schemes merely to protect secret information or messages on the smart card itself, but do not authorize or authenticate a smart card (i.e., do not prevent counterfeiting and cloning of a smart card).

For example, the claimed invention, as defined for example by independent claim 1, provides a method of preventing counterfeiting of a smart card, including:

providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined small number of readings,

wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof;

providing a reader for reading said smart card and including a database holding information related to unauthorized smart cards, said reader being on-line, such that said reader is operatively connected to a network, only when said database of said reader is being updated by said network,

wherein said reader includes a random number generator, which, when a card is read, chooses a pair (a, b) of distinct numbers with a < b between 1 and N,

wherein said smart card carries thereon predetermined N channels as C1, C2, ..., CN, where N is an integer,

wherein each channel Ci, with i equal to 1, 2, ..., N, carries a pair of numbers (hi, li), and

wherein hi is the ith high number and li is the ith low number, wherein said reader obtains a content of only two of said channels, and

periodically communicating, by said reader of said smart card, with a database where a predetermined characteristic of the card is checked (emphasis added).

Thus, the claimed invention complements the conventional smart-card-type of security, which is often all carried on the card itself, by providing extra protection depending

U.S. Application No. 09/685,026
Docket No. YOR920000165US1
(YOR.203)

14

on cryptography, with the cryptographic structure (e.g., a key) not being carried by the card and which cannot be accessed completely by a predetermined small number of readings. Moreover, the cryptographic structure can only be built by whoever emits the card or the agent thereof (e.g., see specification at page 4, lines 9-13).

In this way, the claimed invention, in addition to preventing the creation of false cards different from the legitimate cards (i.e., illegitimate cards), also prevents the fabrication of clones of a given legitimate smart card. That is, the present invention also provides a mechanism of protection designed to prevent and/or discourage both copying and creation of new cards (e.g., see specification at page 4, lines 14-17).

Accordingly, Applicants respectfully submit that it would not have been obvious to combine the cited references in the manner alleged in order to arrive at the claimed invention.

Indeed, the claimed invention has recognized that the unique combination of the features of the claimed invention provides important advantages over the prior art of record, including such teachings as disclosed by each of the individually cited references, Urata, Corcoran, Schneier, and Maillard.

It is noted that the references as a whole must be considered for what they fairly teach to the ordinarily skilled artisan. Moreover, merely identifying individual elements of the claims in separate references is not sufficient to establish the obviousness of the claims. The Office Action must establish a reasonable motivation or suggestion, in the references themselves or in the art in general, for combining the references to arrive at the claimed invention. The mere fact that references could (or can) be combined or modified is not

U.S. Application No. 09/685,026 15
Docket No. YOR920000165US1
(YOR.203)

sufficient to establish *prima facie* obviousness (see M.P.E.P. § 2143.01). There must be a reasonable motivation, in the references themselves or in the art in general, to do that which the patent applicant has done.

Moreover, to render the claims obvious, there must also be a reasonable expectation of success and the prior art references, when combined, must teach or suggest all of the claim limitations (e.g., see M.P.E.P. § 2142). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Applicant's disclosure (see M.P.E.P. § 2143, citing In re Vacek, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

In the present Office Action, the Examiner alleges that Urata teaches a method/computer readable medium for preventing counterfeiting and cloning of smart cards, which includes "providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined small number of readings", citing Urata at column 2, lines 32-52.

The Examiner acknowledges that Urata does not teach that the cryptographic structure can be built only by whoever emits the card or an agent thereof or providing a reader for reading said smart card including a database holding information related to unauthorized smart cards, the reader being on-line, such that the reader is operatively connected to a network, only when the database of said reader is being updated by the network, wherein the reader includes a random number generator, as claimed.

However, the Examiner alleges that Corcoran makes up for some of the deficiencies of Urata by allegedly disclosing that the cryptographic structure can be built only by

U.S. Application No. 09/685,026
Docket No. YOR920000165US1
(YOR.203)

16

whoever emits the card or an agent thereof, citing Corcoran at page 3, third bullet (biometrics or a PIN verify an agent of the card). The Examiner further alleges that Corcoran discloses providing a reader for reading said smart card including a database holding information related to unauthorized smart cards, said reader being on-line, such that said reader is operatively connected to a network, only when said database of said reader is being updated by said network, citing Corcoran at page 3, fourth bullet (discussing obtaining a public key from a database), and that the reader includes a random number generator, citing Corcoran at page 3, second bullet (transmitting random numbers from the card reader to the card). The Examiner also alleges that Corcoran teaches that card readers can be computers in and of themselves or linked to a computer by a connection of some sort, citing Corcoran at page 3 and 4, MORE ABOUT CARD READERS.

The Examiner alleges that it would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof and providing a reader including a database of unauthorized smart cards, said reader being online and connected to a network only when said reader is being updated, as taught by Corcoran, with the system of Urata. The Examiner alleges that it would have been obvious for such modifications because the off-line version of the blacklist provides a listing of all-users who are intruders; the periodic updating allows a newer list of intruders to be known. The Examiner also alleges that the alleged combination would have been obvious because keeping the cryptographic structure secret to only those who emit the card prevents someone from counterfeiting a smart card.

U.S. Application No. 09/685,026
Docket No. YOR920000165US1
(YOR.203)

17

The Examiner also acknowledges that the combination of Urata as modified by Corcoran still does not teach when a card is read, chooses a pair (a, b) of distinct numbers with $a < b$ between 1 and N. However, the Examiner then alleges that Schneier makes up for some of the deficiencies of Urata and Corcoran by allegedly disclosing that when a card is read, chooses a pair (a, b) of distinct numbers with $a < b$ between 1 and N (citing Schneier: a step of an RSA algorithm, choose two prime numbers, page 467).

However, with respect to claim 10 (now incorporated into claim 1), the Examiner further acknowledges that the combination of Urata, Corcoran, and Schneier fail to teach periodically communicating, by the reader of the smart card, with a database where a predetermined characteristic of the card is checked, as claimed.

Therefore, the Examiner turns to a fourth reference, Maillard, to make up for some of the deficiencies of Urata, Corcoran, and Schneier by allegedly disclosing periodically communicating, by the reader of the smart card, with a database where a predetermined characteristic of the card is checked, citing Maillard at column 14, lines 4-6.

The Examiner alleges that it would have been obvious to combine periodically communicating with a database, as allegedly taught by Maillard with respect to a smartcard for a receiver of encrypted broadcast signals, with the alleged combination of Urata, Corcoran, and Schneier, because the periodic check allegedly would ensure that the current card isn't blacklisted.

U.S. Application No. 09/685,026
Docket No. YOR920000165US1
(YOR.203)

18

However, Applicants respectfully submit that it would not have been obvious to combine the cited references in the manner alleged in order to arrive at the claimed invention.

As mentioned above, the mere fact that references could (or can) be combined or modified is not sufficient to establish the obviousness of the claims. Indeed, it is not enough merely to identify (or pick and choose) individual elements from the references and combine them to try to arrive at the claimed invention, with the benefit of Applicants' invention as a guide to such a combination, in order to establish the obviousness of the claimed invention.

Applicant submits that the references themselves do not provide any motivation for combining the respective features of the four cited prior art references to arrive at the unique combination of features recited by the claimed invention.

That is, absent the benefit of Applicant's own disclosure to provide a guide for combining the references (i.e., impermissible hindsight-based analysis), there would be no reason to pick-and-choose the respective features from the four references to arrive at the claimed invention.

In comparison, the claimed invention has recognized that the unique combination of the features of the claimed invention provides the important advantages described above over the prior art of record, including such teachings as disclosed by each of the individually cited references, Urata, Corcoran, Schneier, and Maillard.

Thus, for at least the foregoing reasons, Applicants respectfully submit that it would not have been obvious to combine prior art of record to arrive at the claimed invention.

U.S. Application No. 09/685,026 19
Docket No. YOR920000165US1
(YOR.203)

absent impermissible hindsight based analysis. Accordingly, Applicants submit that the prior art rejections fail to establish the obviousness of the claims as a matter of law.

Applicants also submit that there are elements of the claimed invention which clearly are not disclosed or suggested by the prior art of record, alone or in combination. Thus, Applicants further submit that, as a matter of fact, the alleged combination of references, even if combined in the manner alleged by the Examiner, would not arrive at the claimed invention.

On the other hand, Applicants submit that independent claims 24 and 27 also are patentable over the cited references for somewhat similar reasons as those set forth above.

For example, independent claim 24 recites a method of preventing counterfeiting of a smart card, comprising:

providing a smart card such that none of confidential information and a cryptographic key for authorizing the smart card, is carried on the smart card;

reading said card by a reader such that in each reading, said reader reads only a predetermined small amount of information which makes the card unique (emphasis added).

Independent claim 27 recites a signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for preventing counterfeiting and cloning of smart cards, comprising:

providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined number of readings,

wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof (emphasis added).

U.S. Application No. 09/685,026 20
Docket No. YOR920000165US1
(YOR.203)

As mentioned above, the claimed invention, as defined for example by independent claims 1, 24, and 27, does not merely protect the secret of messages, but instead, authenticates or authorizes a smart card in order to prevent counterfeiting and cloning of the smart card. Thus, Applicants respectfully submit that there is a clear and profound difference between the cited references and the claimed invention.

Applicants submit that the dependent claims also are patentable over Leppek and Maillard by virtue of their respective dependencies, as well as for the additional features recited therein.

For the foregoing reasons, Applicants respectfully submit that neither Leppek nor Maillard, alone or in combination, discloses or suggests all of the features of claims 1, 3, 5-8, and 11-28. Therefore, Applicants respectfully request that the Examiner withdraw this rejection.

III. CONCLUSION

In view of the foregoing, Applicants submit that claims 1, 3, 5-8, and 11-28, all the claims presently pending in the application, are patentably distinct over the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.


U.S. Application No. 09/685,026
Docket No. YOR920000165US1
(YOR.203)

21

The Commissioner is hereby authorized to charge any deficiency in fees or to credit any overpayment in fees to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted.

Date: April 17, 2006



John J. Dresch, Esq.
Registration No. 46,672

Sean M. McGinn, Esq.
Registration No. 34,386

**MCGINN INTELLECTUAL PROPERTY
LAW GROUP, PLLC**
8321 Old Courthouse Road, Suite 200
Vienna, Virginia 22182-3817
(703) 761-4100
Customer No. 21254

CERTIFICATE OF TRANSMISSION

I certify that I transmitted via facsimile to (571) 273-8300 the enclosed Amendment under 37 C.F.R. § 1.111 to Examiner Brandon S. Hoffman, Art Unit 2136, on April 17, 2006.


John J. Dresch, Esq.
Registration No. 46,672
Sean M. McGinn, Esq.
Registration No. 34,386